CLAIMS

1. A circuit design method executed by a computer for designing a processing circuit for applying a plurality of different first processings to predetermined data comprising:

a first step of identifying second processings performing the same processing on the same data in pluralities of second processings forming each of said plurality of first processings and

a second step of designing a processing circuit comprising a first processing circuit shared by said plurality of first processings and performing said second processings identified in said first step and a second processing circuit for performing processings other than said second processings identified in said first step in said pluralities of second processings forming each of said plurality of first processings.

2. A circuit design method as set forth in claim 1, wherein:

said first processings are linear transform processings, and

said second processings are addition.

3. A circuit design method as set forth in claim 1, further comprising, when said plurality of first processings are processings applying first linear

transforms to said predetermined data different predetermined number of times,

a third step of defining a second linear transform combining a number of first linear transforms corresponding to the predetermined number of times of processing for each of the plurality of first processings, and

in said first step, identifying said second processings performing the same processing on the same data among said plurality of second processings forming said second linear transform defined for each of said plurality of first processings at said third step.

4. A circuit design method as set forth in claim 3, further comprising, in said second step, designing said processing circuit so as to perform said plurality of first processings in parallel on said predetermined data based on said second linear transforms defined in said third step.

5. A circuit design method as set forth in claim 3, wherein:

said predetermined data is expressed by a vector by a predetermined base on a predetermined linear space, and

said linear transforms are transforms defined on said linear space.

6. A circuit design method as set forth in claim 3, further comprising, when said predetermined linear space is indicated by the following (3-1), said data "a" of the predetermined data is indicated as the m-th dimension vector by the following (3-4) when using the base shown in the following (3-2) as the predetermined base and said data "a" is indicated as in the following (3-3), said first linear transform is defined as the linear transform D on the linear space shown in the following (3-1), the data "b" of the result of the above plurality of processings is shown as the k-th dimension vector by the following (3-5), and the data bi indicating the results of the processings forming the data "b" shown in the following (3-5) is shown as the di-th dimension vector by the following (3-6),

defining the matrix M comprised by di rows and "m" columns, performing said second linear transforms, and shown by the following (3-7) in said third step and

identifying said second processings performing the same processing on the same data among said plurality of second processings based on the following (3-7) defined in said third step in said first step,

where, "m" and di are integers of 2 or more, the predetermined number of times corresponding to at least one of the above plurality of processings is 2 or

more, and "k" is an integer of 2 or more:

$$\text{Linear space } Fg^m \tag{3-1}$$

$$\{\gamma_1, \gamma_2, \ldots, \gamma_m\} \tag{3-2}$$

$$a=a_1\gamma_1+a_2\gamma_2+\ldots a_m\gamma_m \tag{3-3}$$

$$a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix} \tag{3-4}$$

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{pmatrix} \tag{3-5}$$

$$b_i = \begin{pmatrix} b_{i,1} \\ b_{i,2} \\ \vdots \\ b_{i,di} \end{pmatrix} \tag{3-6}$$

$$M = \begin{pmatrix} D \\ D^2 \\ \vdots \\ D^K \end{pmatrix} \tag{3-7}$$

7. A circuit design method as set forth in claim 6, wherein when using the base shown by the following (3-8) as said predetermined base and said data "a" is shown as in the following (3-9), said data "a" is shown by the following (3-10) as an m-th dimension vector:

$$\{1, \gamma, \gamma^2, \ldots, \gamma^{m-1}\} \qquad (3\text{-}8)$$

$$a = a_0 + a_1\gamma + a_2\gamma^2 + a_3\gamma^3 + \ldots + a_{m-1}\gamma^{m-1} \qquad (3\text{-}9)$$

$$a = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{m-1} \end{pmatrix} \qquad (3\text{-}10)$$

8. A circuit design method as set forth in claim 6, wherein said third step defines said matrix M comprised of said matrixes D for performing γ^r-times multiprocessing based on the dimension γ on said linear space.

9. A circuit design apparatus of a processing circuit for applying a plurality of different first processings to predetermined data comprising:

a first means for identifying second processings performing the same processing on the same data in pluralities of second processings forming each of said plurality of first processings and

a second means for designing a processing circuit comprising a first processing circuit shared by said plurality of first processings and performing said second processings identified by said first means and a second processing circuit for performing processings other than said second processings identified by said

first means in said pluralities of second processings forming each of said plurality of first processings.

10. A program executed in a circuit design apparatus of a processing circuit for applying a plurality of different first processings to predetermined data comprising:

a first routine of identifying second processings performing the same processing on the same data in pluralities of second processings forming each of said plurality of first processings and

a second routine of designing a processing circuit comprising a first processing circuit shared by said plurality of first processings and performing said second processings identified in said first routine and a second processing circuit for performing processings other than said second processings identified in said first routine in said pluralities of second processings forming each of said plurality of first processings.